Bandit

00: ZjLjTmM6FvvyRnrb2rfNWOZOTa6ip5If

Readme

01: 263JGJPfgU6LtdEvgfWU1XP5yac29mFx

./- to allow for use of dash

02: MNk8KNH3Usiio41PRUEoDFPqfxLPlSmx

cat ./--spaces\ in\ this\ filename--

03: 2WmrDFRmJIq3IPxneAaMGhap0pFhF3NJ

Ls, ls -a, cat …Hiding-From-You

04: 4oQYVPkxZOOEOO5pTW81FB8j8lxXGUQw

Brute force ls and cat

Note: file * | grep text

05: HWasnPhtq9AVKe0dmk45nxy20cvUa6EG

find . -type f -size 1033c -exec file {} ; | grep text | grep -v exe

06: morbNTDkSW6jIlUc0ymOdMaLnOlFVAaj

Notes: **bandit6@bandit**:**~**$ find / -user bandit7 -group bandit6 -size 33c 2>/dev/null

2>/dev/null suppresses the denied perms ones

07: dfwvzFQi4mU0wfNbFOe9RoWskMLg7eEc

grep “word” data.txt (-i added case insensitive)

08: 4CKMh1JI91bUIZZPXDqGanal4xvAg0JM
aight this is redirect

> > sends to file < reads from one

putting a number before it allows for you to label your streams
for example:

```
ls -l video.mpg blah.foo 2> errors.txt
```

piping uses | to send to another program. for example:
ls | head -3 | tail -1
head takes top 3, tail returns the 3rd from that list

In this example we are sorting the listing of a directory so that all the directories are listed first.

```
ls -l /etc | tail -n +2 | sort
drwxrwxr-x 3 nagios nagcmd 4096 Mar 29 08:52 nagios
drwxr-x--- 2 news news 4096 Jan 27 02:22 news
drwxr-x--- 2 root mysql 4096 Mar 6 22:39 mysql
...
```

In this example we will feed the output of a program into the program less so that we can view it easier.

```
ls -l /etc | less
(Full screen of output you may scroll. Try it yourself to see.)
```

Identify all files in your home directory which the group has write permission for.

```
ls -l ~ | grep '^.....w'
drwxrwxr-x 3 ryan users 4096 Jan 21 04:12 dropbox
```

Create a listing of every user which owns a file in a given directory as well as how many files and directories they own.

```
ls -l /projects/ghosttrail | tail -n +2 | sed 's/\s\s*/ /g' | cut -d ' ' -f 3 | sort | uniq -c
8 anne
34 harry
37 tina
18 ryan
```

>

Save output to a file.

>>

Append output to a file.

<

Read input from a file.

2>

Redirect error messages.

|

Send the output from one program as input to another program.

Streams

Every program you may run on the command line has 3 streams, STDIN, STDOUT and STDERR.

problem: awk '{count[$0]++} END {for (line in count) if (count[line]==1) print line}' data.txt does this with no sorting needed

> 09: FGUW5ilLVJrxX9kMYMmlN4MgbpfMiqey

grep -E "[1]+" data.txt
^start of line
[=]+ is one or more of this character

strings data.txt worked

10: dtR173fZKb0RRsDFSGsg2RWnpNVj3qRr
base64 encoding
base64 -d encoded.txt

11: 7x16WNeHIi5YkIhWsfFIqoognUTyj9Q4
TR13 rotation
tr 'A-Za-z' 'N-ZA-Mn-za-m' < data.txt

12:FO5dwFsc0cbaIiH0h8J2eUks2vdTDwAn
repeated decoding
Useful commands:

- `base64 -d file` → decode base64
- `xxd -r` → reverse hex dump
- `zcat` / `gzip -d` → decompress gzip
- `bzip2 -d` → decompress bzip2
- `tar -xf` → extract tar archive
- over and over until you get the flag

13: MU4VWeTyJk8ROof1qqmcBPaLh7lDCPvS
make it work with ssh -p 2220 -i (sshkey file) bandit14@bandit.labs.overthewire.org

instead of a password, you are given a private key (sshkey.private)

- You must connect to the next level with SSH using this key.
- 14: 8xCjnmgoKbGLhHFAZlGE5Tmu4M2tKJQo
  ```
  nc localhost 30000 currpassword
  ```
  nc allows you to connect with tcp directly here

15: kSkvUpMQ7lBYyCM4GBPvCvT1BfWRy0Dx

```
openssl s_client -connect localhost:30001
```

its the same was level 14 but with ssl/lts instead of plain tcp

```
nmap -p 31000-32000 -sV localhost
```

---

1. = ↩